-----Original Message-----
**From:** Corbin, Barbara Ms USADTC [mailto:barbara.corbin@us.army.mil]
**Sent:** Friday, March 12, 2004 7:22 AM
**To:** Nieves, Ariel; Kodadek, Bill - Contractor.Cobro; Gonzales, Carmela; Charles D. Wood (E-mail); Hall, Cheryl L Ms. RTTC; Andrus, Dennis D.; DP-IT; Anderson, Eric; Johnson, Eric; Grace Anchondo (E-mail); McShane, James (Contractor); James R Neufeld (E-mail); Josie Nesiba (E-mail); Huber, Ken; Kevin Dorsey (E-mail); Poole, Jeff W Mr. RTTC; Windsor, Ruthie; Sharon Reese (E-mail)
**Subject:** FW: Win2k3 has just completed FIPS 140-2
**Importance:** Low

-----Original Message-----
**From:** Davis, Michael P Mr USADTC
**Sent:** Thursday, March 11, 2004 12:16 PM
**To:** TC CIO/IMO
**Cc:** Roller, Thomas Mr USADTC; Haire, Richard; Little, Robin; Corbin, Barbara Ms USADTC; Bench, Evelyn A.
**Subject:** FW: Win2k3 has just completed FIPS 140-2
**Importance:** Low
All,

Please pass along to all appropriate personnel within your organizations.

Windows Server 2003 is now approved for general deployment, including in cases where encryption is necessary. A revised TECHCON from NETCOM indicating same is pending; the previous guidance is attached, but disregard any references to restrictions in deployment.

v/r,
Mike Davis
DTC IT Division

-----Original Message-----
**From:** walt williams [mailto:walt.williams@us.army.mil]
**Sent:** Thursday, March 11, 2004 12:02 PM
**To:** Cassil, Cindy Ms ATEC; King, Federica MAJ ATEC; Newton, Richard Mr. ATEC; Haire, Richard; Davis, Michael P Mr USADTC; Sheppard, Cindy Ms. OTC
**Subject:** FW: Win2k3 has just completed FIPS 140-2
**Importance:** Low

Hot off the press. All three modules within Windows 2003 crypto have now been approved by NSA. This will clear the way for wholesale deployment.

walt

**From:** Keith Nielsen [mailto:keithnie@microsoft.com]
**Sent:** Thursday, March 11, 2004 10:42 AM

**Encl 1**

**Subject:** Win2k3 has just completed FIPS 140-2
**Importance:** Low

FYI - Finally - It should be posted on the NIST Website within a week.

**Windows Server 2003 Kernel Mode Cryptographic Module (FIPS.SYS) by Microsoft Corporation Cert 405**

Keith Nielsen
US Army Team Architect
keithnie@microsoft.com
202-669-4044

**DEPARTMENT OF THE ARMY**
**UNITED STATES ARMY NETWORK ENTERPRISE TECHNOLOGY COMMAND/**
**9th ARMY SIGNAL COMMAND**
**2133 CUSHING STREET**
**FORT HUACHUCA, ARIZONA 85613-7070**

REPLY TO
ATTENTION OF:

NETC-EST-G (25-1a)

~ 8 SEP 2003

MEMORANDUM FOR SEE DISTRIBUTION

SUBJECT: NETCOM TECHCON Implementation Memorandum Number 2003-003

1. Reference, ARMY NETOPS CONOPS Version 1.0, approved by CIOEB, 29 Oct 02.

2. IAW reference, NETCOM is responsible to exercise TECHCON for all organizations that operate and maintain portions of the Army Enterprise Infostructure (AEI). NETCOM TECHCON Implementation Memorandum Number 2003-003, at enclosure, defines the NETCOM/9th ASC position for implementing Windows 2003 Server within AEI, until such time as Federal Information Processing Standards (FIPS) 140-2 certification has been granted by National Institute of Standards and Technology (NIST).

3. NETCOM TECHCON Implementation Memorandum Number 2003-003 provides the basis for implementing limited deployment of Windows Server 2003 on Army Networks. This TECHCON provides the parameters under which Windows 2003 Server can be deployed until FIPS 140-2 certification has been granted for Windows Server 2003 by NIST. The intent is to avoid delays in the uses of Windows 2003 servers on the Army Networks where possible in preparation for Windows 2003 Active Directory.

4. The NETCOM/ESTA POC for this action is Robert Bachert, DSN 821-1855, or commercial (520) 533-1855, email address Robert.Bachert@us.army.mil

Encl

Michael Thompson, COL, Dep Dir
for JOE C. CAPPS
Director, Enterprise Systems
Technology Activity

DISTRIBUTION:
DIRECTOR,
USAR, RCIO, NETC, Fort McPherson, GA 30330-5000
ARNG, RCIO, 1411 Jefferson Davis Highway, Arlington, VA 22202-3231
CFSC, RCIO, Alexandria VA 22302-5000
Corps of Engineers (COE), RCIO, 441 G Street NW, Washington, DC 20314-1000
MEDCOM, RCIO, 5109 Leesburg Pike, Falls Church, VA 22041
USAREUR, RCIO, CMR 420, Box 697 APO AE 09063

DISTRIBUTION (CONT)
Korea RCIO, Seoul, Korea APO AP 90625-0044
USAPAC RCIO, Fort Shafter, HI 96858-5100
Southeast RCIO, NEC-SSE-D, 1777 Hardee Ave., SW, Fort McPherson, GA 30330-1062
Southwest RCIO, NETC-SSW-D, Bldg 4011, 1750 Greeley Road, Fort Sam Houston, TX 78234
Northwest RCIO, NETC-SNW-D, 1 Rock Island Arsenal, Rock Island Arsenal, IL 61299-6800
Northeast RCIO, NETC-SNE-D, 90 Ingalls Road, Bldg 100, Fort Monroe, VA 23651
IMCEN, Office of the Director, 6602 Army Pentagon, Washington, DC 20310-0660

HQ USANETCOM STAFF,
DIRECTOR,
ANOSC, NETC-AND, Fort Huachuca, AZ 85613-7070
HQ NETCOM, TNOSC, Fort Huachuca, AZ 85613-7070
Commander, 516th Sig Bde, TNOSC, PAC-TNOSC, Bldg 520, Rm C11, Fort Shafter, HI 96858
Commander, 5th Sig Cmd, TNOSC, CMR-421, ANOSCE, APO AE 09056
Commander, 1st Sig Bde, TNOSC, APO AP 96218
335th TSC Fwd, SWA TNOSC, SWA-TNOSC, Camp Doha, KU APO AE 09889-9900
Commander, 93d Sig Bde, S-TNOSC, Fort Gordon, GA 30905

ACofS, G2
ACofS, G3

CF:
CIO/G6, BG Ponder, 107 Army Pentagon, Washington, DC 20310-0107
CIO/G6, COL Barnette, 107 Army Pentagon, Washington, DC 20310-0107
PEO EIS, Mr. Carroll, 9350 Hall Road, Fort Belvoir, VA 22060-5526
PM EI, COL Hogan, 9350 Hall Road, Fort Belvoir, VA 22060-5526
CDR ISEC, COL Brown, ATTN: AMSEL-IE-CO, Fort Huachuca, AZ 85613-5300
SIGCEN, ATZH-CDM, Fort Gordon, GA 30905
Installation Management Agency, 2511 Jefferson Davis Highway, Arlington, VA 22202-2511
USANETCOM/9th ASC, ESTA Sr. LNO to NCR, Ms. Amy Harding, 107 Army Pentagon, Washington, DC 20310-0107

| | | |
|---|---|---|
| NETC-EST-P | NETC-EST-A | NETC-EST-C |
| NETC-EST-E | NETC-EST-I | NETC-EST-K |
| NETC-EST-S | NETC-EST-T | NETC-EST-V |

# NETCOM/9th ASC TECHCON Implementation Memorandum

U.S. ARMY ENTERPRISE SYSTEMS TECHNOLOGY ACTIVITY
Fort Huachuca, AZ 85613-7070

NETCOM/9th ASC TECHCON

Implementation Memorandum Number 2003-003

## Subject: GUIDANCES FOR IMPLEMENTING WINDOWS SERVER 2003 ACROSS THE ARMY ENTERPRISE

**Date of Issue: 22 September 2003**

**Date of Required Compliance: N/A**

**Date of Expiration/Suppression: Until FIPS 140-2 certification has been granted**

Encl

1. The purpose of this NETCOM TECHCON Implementation Memorandum is to provide guidelines for implementing Windows Server 2003 across the Army Enterprise. On April 24, 2003 Microsoft announced the general availability of Windows Server 2003. Microsoft has been working with NETCOM to satisfy requirements to allow use of Windows Server 2003 Active Directory on Army Networks. This guidance provides the basis for limited deployment of Windows Server 2003 on Army Networks.

2. Microsoft has contracted for Federal Information Processing Standards (FIPS) 140-2 evaluations of the Windows Server 2003 cryptographic modules and their contracted laboratory has submitted test data and validation certificates to National Institute of Standards and Technology (NIST) for evaluation. Until NIST has completed its review and issued FIPS 140-2 certification for the Windows Server 2003 Cryptographic modules, Army activities may not rely on Windows Server 2003 crypto to protect sensitive but unclassified (SBU) or higher sensitivity data. The Windows Server 2003 services using the cryptographic modules are Internet Explorer (IE), Internet Information Server (IIS), SCHANNEL (used for SSL & TLS), Encrypting File System (EFS), Remote Desktop Protocol (RDP), SQL- Tabular Data Stream (TDS), EFS and Internet Protocol (IP) Security (IPSec). The best-case scenario for completion of Windows Server 2003 FIPS 140-2 validation is during the October to early November 2003 time frame.

3. Until such time as FIPS 140-2 certification has been granted for Windows Server 2003 by NIST, Windows Server 2003 may not be used in production on Army networks if any of the services listed above are required to protect SBU or higher sensitivity information. Army activities may however, proceed with their plans to test and evaluate Windows Server 2003.

4. The following guidelines are provided for deploying Windows 2003 Server without the use of cryptographic modules. Windows Server 2003 can be deployed as a member server within the NT4.0 or Windows 2000 (Win2K) Active Directory (AD) environment (Note, the Win2K AD usage must be part of an approved Forest by the AEIT CCB.) If used as a Domain Controller (DC) within the AD infrastructure prior to completion of Windows 2003 FIPS 140-2 validation, you will be required to use the operating system (OS) cryptographic modules within Win2k or XP (or a 3rd party) that has been FIPS 140-1 validated. One scenario would be to use WIN2K vice Windows 2003 servers to encrypt DC related traffic between AD sites. Another would be an Army Community of Information Network (COIN) that currently has deployed a FIPS 140-1 validated method (i.e. virtual private network (VPN) for securing DC-to-DC traffic. The intent is to avoid delays to the use of Windows 2003 servers if there is no reliance on the cryptographic modules that are in the process of FIPS 140-2 validation.

5. Regional Chief Information Offices (RCIOs) are required to review and approve all Windows 2003 server deployments in their regions or functional areas; RCIO approval should be based on validation that no reliance is required on the crypto

algorithms noted above until FIPS 140 is approved. RCIOs will not provide approval for any Windows 2003 deployments that are not in compliance with the guidance contained herein.

6. On August 7, 2003 the National Security Agency (NSA) published Information Assurance Advisory No. IAA-006-2003 regarding Windows Server 2003. The NSA will not be publishing a separate Security Guide for Windows Server 2003, and recommends use of the Microsoft "Windows Server 2003 Security Guide", with its associated tools and templates in determining appropriate security settings and configurations.

7. Licenses for Windows Server 2003 must be acquired via the procedures for the Army Enterprise Agreement.
http://pmscp.monmouth.army.mil/standard/standard_policy.htm